PERFORMANCE AUDIT
OF THE

AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF STATE AND
DEPARTMENT OF INFORMATION TECHNOLOGY

August 2004

"...The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof."

– Article IV, Section 53 of the Michigan Constitution

Audit report information may be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Automated Information Systems

Department of State and Department of Information Technology

Report Number:
23-590-03

Released:
August 2004

The Department of State has developed and operates large complex information systems to manage driver and vehicle information, vehicle-licensing records, vehicle violations, and fee collections. The Department collects nearly $2 billion in revenue each year. This money is used for a variety of purposes as required by law. The Department of Information Technology is responsible for maintaining and supporting the information technology (IT) infrastructure for the Department of State.

Audit Objective:

To assess the effectiveness of the general controls over security, access, program and data changes, segregation of duties, and service continuity that support mainframe information systems.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Conclusion:

The Department of State's and the Department of Information Technology's general controls over security, access, program and data changes, segregation of duties, and service continuity that support mainframe information systems were not effective. As a result, there was a significant risk that unauthorized access to the Departments' mainframe information systems could compromise the confidentiality, integrity, and availability of Department of State information resources.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Material Conditions and Agency Responses:

Comprehensive Information Systems Security Program

The Departments had not fully implemented a comprehensive information systems security program (Finding 1).

Agency Response: The Departments will continue their efforts to fully implement a comprehensive information systems security program consistent with the objectives set forth in the *Secure Michigan Initiative* issued in January 2003.

Organizational Controls

The Departments had not established effective organizational controls to support mainframe information systems (Finding 2).

Agency Response: The Departments continue to improve the effectiveness of organizational controls. The Departments informed us that since the completion of the audit, responsibilities and expectations related to IT management have been formalized into an agreement between the two Departments and a new security-focused function has been established at the Department of State. Additional efforts are also underway to further implement widely accepted control objectives into building and managing systems.

Access to System Account

The Departments did not control access to a critical production system account and job-scheduling utility (Finding 3).

Agency Response: The Departments informed us that they have taken steps to limit access to the critical production system account and job scheduling utility and have developed plans for implementing additional security procedures to protect against this access risk.

Access to Mainframe Information System Files

The Departments had not established effective access controls over mainframe information system files (Finding 4).

Agency Response: The Departments have plans to establish new controls to limit access to mainframe information system files. Despite the risks associated with the current arrangement for managing access controls, the Departments are not aware of any instances in which the confidentiality, integrity, or availability of information system resources was inappropriately compromised.

Access to Mainframe Information Systems

The Departments had not established effective access controls over mainframe production information systems (Finding 5).

Agency Response: The Departments informed us that they have already taken steps to establish effective access controls through a comprehensive analysis and updating of access rights into the mainframe production systems. Additional policies and procedures will also be developed to further protect against this access risk.

Program and Data Change Controls

The Departments had not established effective program and data change controls (Finding 6).

Agency Response: The Departments informed us that they have already implemented revised procedures for "project-related" program releases and will further refine procedures to provide sufficient control over other program and data changes.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

August 31, 2004

The Honorable Terri Lynn Land
Secretary of State
Treasury Building
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
Landmark Building
Lansing, Michigan

Dear Secretary Land and Ms. Takai:

This is our report on the performance audit of the Automated Information Systems, Department of State and Department of Information Technology.

This report contains our report summary; description of agency; audit objective, scope, and methodology and agency responses; comment, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

The agency preliminary responses were taken from the agencies' responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Thomas H. McTavish, C.P.A.
Auditor General

This page left intentionally blank.

TABLE OF CONTENTS

AUTOMATED INFORMATION SYSTEMS
DEPARTMENT OF STATE AND
DEPARTMENT OF INFORMATION TECHNOLOGY

Description of Agency

Department of State

The mission* of the Department of State is to continually improve customer service using innovation and new technology. The Department will serve the citizens of Michigan with programs designed to enhance driver safety, protect automotive consumers, and ensure the integrity of the motor vehicle administration system and the Statewide elections process.

The Department of State has developed and operates large complex information systems to manage driver vehicle information, vehicle-licensing records, vehicle violations, and fee collections.

The Department collects nearly $2 billion in revenue each year. This money is distributed primarily among the Michigan Transportation Fund, the School Aid Fund, and the General Fund and is used for a variety of purposes as required by law.

Executive Order No. 2001-3 created the Department of Information Technology and gave it responsibility for Statewide information technology staff and projects. Pursuant to the Executive Order, the Department of State transferred staff performing information technology functions to the Department of Information Technology.

In fiscal year 2002-03, $21,044,700 was transferred from the Department of State's appropriations to the Department of Information Technology for information technology related services.

Department of Information Technology

The Department of Information Technology is responsible for maintaining and supporting the information technology infrastructure for the Department of State. In addition, the Department of Information Technology provides technical support for Department of State application development and maintenance, database management, and help desk services.

Within the Department of Information Technology, there are three organizational units that provide direct and indirect support and services to Department of State resources

* *See glossary at end of report for definition.*

on the State's mainframe system. These organizational units include Data Center Operations, Distributed Processing Operations, and Agency Support Services for the Department of State:

a. Data Center Operations

Data Center Operations is responsible for providing centralized data processing services for all State agencies. These services include operational and technical support for a variety of mainframes systems. Data Center Operations also provides agencies with a complex security system to control access to mainframe resources. Data Center Operations' security system allows agency security administrators to define authorized individuals and grant appropriate access to information resources.

b. Distributed Processing Operations

Distributed Processing Operations is responsible for providing centralized job scheduling and processing for all State agencies on the State's mainframe environment.

c. Agency Support Services for the Department of State

Agency Support Services for the Department of State is the liaison between the Department of Information Technology and the Department of State. The role of this unit is to work with the Department of State to achieve agency information technology goals. Agency Support Services for the Department of State provides services that include system development, application programming, database management, and information security for mainframe information systems.

Audit Objective, Scope, and Methodology and Agency Responses

Audit Objective

The objective of our performance audit* of the Automated Information Systems, Department of State and Department of Information Technology, was to assess the effectiveness* of the general controls over security, access, program and data changes, segregation of duties, and service continuity that support mainframe information systems.

Audit Scope

Our audit scope was to examine the information processing and other records of the Department of State's and the Department of Information Technology's mainframe information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of the Departments' information processing and other records primarily for the period January 2000 through November 2003. Our work was performed between April and November 2003. To accomplish our audit objective, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We conducted a preliminary review of the information processing functions that support the Department of State's mainframe information systems. These functions include management and organization, information security, program and data changes, backup and recovery, and access to information systems. We used this analysis to determine the extent of our detailed analysis and testing.

* *See glossary at end of report for definition.*

2. Detailed Analysis and Testing Phase

   We performed an assessment of internal control* pertaining to the general controls that support the Department of State's mainframe information systems. Specifically:

   a. We identified and analyzed controls over the management and organization of the information technology (IT) functions that support mainframe information systems. We obtained an understanding of how the various roles and responsibilities for the management of IT were assigned. We assessed the segregation of responsibilities between certain IT functions and business owners.

   b. We interviewed the information security officer and reviewed security policies and procedures to obtain an understanding of the security program.

   c. We examined and tested controls over program changes, file security, administration of security systems, and critical system utilities that support job scheduling and program changes.

   d. We reviewed mainframe backup and recovery strategies.

   e. We examined and tested controls over access to mainframe information systems.

   f. We did not examine and test controls over the mainframe operating system and database management system.

3. Evaluation and Reporting Phase

   We evaluated and reported on the results of the detailed analysis and testing phase.

Agency Responses

Our audit report contains 6 findings and 6 corresponding recommendations. The agency preliminary responses indicated that the Department of State and the Department of Information Technology agree with the findings and has partially complied or will comply with the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require the Department of State and the Department of Information Technology to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENT, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF GENERAL CONTROLS

COMMENT

Background: General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They include an entity wide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.

The purpose of establishing general controls is to safeguard data, protect computer application programs, prevent unauthorized access to system software, and ensure continued computer operations in case of unexpected interruptions. The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. Without effective general controls, existing application controls may be rendered ineffective by circumvention or modification.

Pursuant to Executive Order No. 2001-3, the Department of State transferred its information technology (IT) functions to the newly established Department of Information Technology. Subsequent to this transition, the Department of Information Technology had not significantly revised the processes and controls of the IT functions that it had inherited. Consequently, the processes and controls that we reviewed during our fieldwork were designed and put in operation by the Department of State before transferring its IT functions to the Department of Information Technology.

Audit Objective: To assess the effectiveness of the general controls over security, access, program and data changes, segregation of duties, and service continuity that support mainframe information systems.

Conclusion: The Department of State's and the Department of Information Technology's general controls over security, access, program and data changes, segregation of duties, and service continuity that support mainframe information systems were not effective. Our assessment disclosed six material conditions* related to comprehensive information systems security program, organizational controls, access to system account, access to mainframe information system files, access to mainframe information systems, and program and data change controls.

* *See glossary at end of report for definition.*

As a result, there was a significant risk that unauthorized access to the Departments' mainframe information systems could compromise the confidentiality, integrity, and availability of Department of State information resources.

We reported to the Departments' managements the detailed results of our review. This report summarizes the material conditions we identified and recommendations we made.

FINDING

1. Comprehensive Information Systems Security Program

The Department of State and the Department of Information Technology had not fully implemented a comprehensive information systems security program. Without a fully operational security program, management cannot effectively maintain the confidentiality, integrity, and availability of mainframe information system resources.

In May 2002, the director of the Department of Information Technology took a major step in addressing the security needs of the State by appointing the first chief information security officer (CISO) to oversee the security of State government information systems and networks. The next major advancement toward the creation of a comprehensive security program was in January 2003 when the CISO published the *Secure Michigan Initiative*. The *Secure Michigan Initiative* summarizes the current assessment of threats and risks, options for risk mitigation, and recommendations for improving security.

Our review of the security over the Department of State's mainframe information systems indicates that both the Department of State and the Department of Information Technology should continue their efforts to implement the recommendations outlined in the *Secure Michigan Initiative* and address the control weaknesses identified in this report:

a. The Departments have not fully implemented the recommendations of the *Secure Michigan Initiative*. These include recommendations to ensure that the financial commitment for securing the State of Michigan is built into the budget approval process and also to ensure that the CISO's authority to enforce security policy compliance is established through an executive order. The CISO warns that "If the recommendations in this report [*Secure Michigan*

Initiative] are not acted upon, state government IT systems face very serious consequences and risks."

b. As discussed in Findings 2 through 6, the Departments had not established effective organizational controls to support mainframe information systems, did not control access to a critical production system account, had not established effective access controls over mainframe information system files, had not established effective access controls over mainframe production information systems, and had not established effective program and data change controls.

c. The Departments had not assessed the risks to major access control systems and critical application support utilities or conducted recent tests of disaster recovery plans for critical mainframe information systems.

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology continue their efforts to fully implement a comprehensive information systems security program.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding for the time period covered by this performance audit and will continue with their efforts to fully implement a comprehensive security program. As noted by the Office of the Auditor General, in January 2003, the Department of Information Technology initiated the *Secure Michigan Initiative*, which identifies a comprehensive information security program including six high priority steps to address the Departments' primary information system security risks. As part of this program, in December 2003, the Department of State established an information security function which is intended to complement the efforts of the Department of Information Technology. Also, the two Departments are proceeding with the development of a new automated information system intended to support Department of State business processes into future years. A mandatory requirement of this new information system is security over the customers' records. The implementation phase of this project is expected to begin in fiscal year 2004-05.

FINDING

2. Organizational Controls

The Department of State and the Department of Information Technology had not established effective organizational controls to support mainframe information systems. This has resulted in material control weaknesses throughout the IT development function that adversely affect the integrity of the Department of State's information systems.

During our audit, we noted that the cause of many of our audit findings were related to incompatible* job assignments or insufficient expertise in control standards and techniques and information security. We noted the following weaknesses in organizational controls:

a. The Departments assigned incompatible job functions to IT development staff*.

IT development staff were acting as the Department of State's information security officer, administering security and access to the job-scheduling utility, maintaining access to the production system account and other privileged access rights, and managing program code libraries. As a result, IT development staff had the opportunity to gain unauthorized access and use of confidential information or commit fraudulent activity that would likely go undetected.

The Department of Information Technology should reassign IT operational support and security functions to individuals independent of IT development.

b. The Departments had not formally adopted IT control objectives and standards to effectively manage their information systems resources.

Generally accepted IT control objectives and standards provide a practical framework for identifying, understanding, assessing, and implementing effective IT controls into business processes and information systems. The identification and selection of suitable controls are critical to the cost-effective management of risk stemming from the evolving use of IT.

* *See glossary at end of report for definition.*

In 1999, the Department of Management and Budget (DMB) revised its *Evaluation of Internal Controls - A General Framework and System of Reporting**. The revised general framework explained the issues for controlling the use of IT.

To address these issues, DMB recommended that department management, together with department internal auditors, consider the use of the Control Objectives for Information and Related Technology (COBIT) control framework*. COBIT offered management and internal auditors a framework to build and maintain quality systems, but also serves as the criteria for evaluating management's performance at efficiently building quality systems to support departmental business requirements.

The DMB recommendation to use the COBIT control framework was a significant step toward improving the State's overall system of internal controls. However, the use of COBIT was not mandated in the general framework. Consequently, the Departments' use of COBIT has been limited to primarily as an evaluation tool.

The Departments' managements should formally adopt and integrate the COBIT framework in their efforts to build, manage, and maintain quality information systems.

c. The Departments lacked sufficient technical training to effectively manage their information systems security needs.

The configuration of the Department of Information Technology's mainframe security system is highly complex. This highly complex system requires that the Departments assign individuals to information security that possess and maintain the needed knowledge, skills, and ability to effectively manage information security.

Without a comprehensive and detailed understanding of the mainframe's file system, database management system, user account system, job scheduling system, program change control system, and transaction control system, the

** See glossary at end of report for definition.*

Departments' information security function cannot effectively maintain security over critical information resources.

d. The Departments did not have effective controls to monitor privileged activity and security. Consequently, inappropriate or unauthorized access may be mistakenly or intentionally granted to critical mainframe information resources.

   We noted that management reviewed little if any of the privileged activity of security administrators or those individuals responsible for processing requests to access Department of State information systems. Privileged activity includes setting up security administrators and usercode and access rights managers and granting access to high-risk transaction code lists.

   Privileged access to mainframe information resources is necessary for the ongoing maintenance and support of Department of State mainframe information systems. Management should have controls in place that monitor the use of privileged access and ensure that it is appropriate and authorized.

e. The Departments had not established a service level agreement. Without an agreement that clearly defines responsibilities, expectations, and processing needs, the Department of Information Technology is less effective in providing secure and reliable service to the Department of State.

   Executive Order No. 2001-3 calls for the development of service-level agreements to ensure that quality services are delivered on schedule and within budget. Service level agreements establish responsibility for various control functions, i.e., information security, application program, data and database access, and disaster planning. The agreements also serve as a basis for communicating future processing requirements.

f. The Departments did not establish comprehensive policies and procedures to manage certain IT security functions. This condition presents a high risk that responsibility for critical functions will not be assigned to appropriate personnel or properly and consistently carried out.

   We noted that policies and procedures were not developed for administering access to the mainframe security system, to databases and disk files, and to the Department of State mainframe information systems.

Establishing comprehensive policies and procedures will provide the Departments with the means to comply with Sections 18.1483 - 18.1489 of the *Michigan Compiled Laws.*

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective organizational controls to support mainframe information systems.

AGENCY PRELIMINARY RESPONSE

Both the Department of State and the Department of Information Technology agree with the finding for the period covered by the audit. The Departments informed us that since November 2003 organizational controls have been enhanced as the Department of State has now established an information security function and a service level agreement has been finalized that identifies the conditions and expectations of the two Departments regarding the delivery of IT services.

In addition, the Department of State and the Department of Information Technology will plan to continue to use widely accepted control objectives in evaluating IT activities and will work to further integrate these concepts into building and managing systems, formalizing additional policies and procedures when needed. The Departments will also continue to explore and offer training opportunities to better enable staff with necessary skills associated with information system security and controls.

FINDING

3. Access to System Account

The Department of State and the Department of Information Technology did not control access to a critical production system account and job-scheduling utility. Unauthorized access and use of the production system account and job-scheduling utility could compromise the confidentiality, integrity, and availability of critical production mainframe information resources.

One of the primary means of controlling access to mainframe information resources is by assigning ownership of the resource. The Department of Information Technology's Data Center Operations establishes a unique production

system account for each State agency that it serves. Agencies use their production system account to control access to their production resources. It is the responsibility of each State agency to protect information resources and control access to the production system account.

Access to the production system account must be restricted and closely monitored. Access to this account should be limited to operational support staff that are responsible for scheduling production jobs.

Our review of access to the Department of State's production system account disclosed that access was not restricted to operational support personnel. Further, the Departments had not established effective controls to administer access to a critical job-scheduling utility.

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology control access to the critical production system account and job-scheduling utility.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with this finding and have informed us that they have taken steps to limit access to the critical production system account and job-scheduling utility to appropriate staff. Additional security procedures to protect against this access risk will be accomplished by December 2004.

FINDING

4. Access to Mainframe Information System Files

The Department of State and the Department of Information Technology had not established effective access controls over mainframe information system files. Consequently, the integrity and security of the Department of State's information systems cannot be maintained.

The Department of State stored thousands of files on the Department of Information Technology's mainframe computer system. These files support the Department of State's major licensing and vehicle registration systems as well as

financial and other information systems. We reviewed the access controls for these files and identified the following material conditions:

a. The Departments had not secured the 9 mainframe production databases from unauthorized access at the operating system level. We identified inappropriate access rights granted to nonoperational support staff and noted the absence of access authorization forms for approximately 95% of the individual accounts.

b. The Departments had not established effective access controls over mainframe application files.

   These application files contain data, program code, and process rules. Our analysis indicates that all production and development files were vulnerable to unauthorized access. Effective access controls are critical to maintaining the integrity and confidentiality of the Department of State's information systems that may contain confidential driver and licensing information.

DMB Administrative Guide procedure 1310.02 requires that production programs and data files be protected from unauthorized access. In addition, files stored in the development environment must also be protected because confidential driver and licensing information could be disclosed or unauthorized code or data could be introduced into production information systems from the development environment.

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective access controls over mainframe information system files.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding and will establish new controls to limit the access to confidential mainframe information system files by December 2004. Despite the risks associated with having this monitored by IT staff during this transition period, the Departments are not aware of any instances in which the confidentiality, integrity, and availability of information system resources was inappropriately compromised.

FINDING

5. Access to Mainframe Information Systems

The Department of State and the Department of Information Technology had not established effective access controls over mainframe production information systems. Without effective access controls, the Departments cannot maintain the integrity of mainframe information systems.

A basic management objective for any organization should be the protection of its information systems and critical data from unauthorized access. Organizations accomplish this objective in part by establishing controls that limit access to only authorized users. Our review of the Departments' efforts to control access to mainframe information systems disclosed:

a. The Departments had not developed written policy and procedures that defined how access was to be granted, who should be allowed access, and the risks associated with granting certain access rights to the Department of State mainframe information systems.

   DMB Administrative Guide procedure 1310.02 states that security requirements and procedures must be documented and approved by management for each application system.

b. The Department of State had not assessed the risks related to transactions used to access its mainframe information systems.

   Risk assessments are important because they help ensure that significant threats and vulnerabilities are identified and considered when decisions are made regarding which risks to accept and which risks to mitigate through security controls.

c. The Departments granted IT development staff extensive and inappropriate access to the Department of State's mainframe information systems.

   IT development staff transferred from the Department of State were allowed to retain their extensive access. However, the Department of Information Technology did not grant new IT development staff extensive access to mainframe information systems.

It is a generally accepted control objective that management should restrict IT development staff's access to production information resources. IT development staff possess a detailed understanding of the information systems as well as the controls over those systems. Granting IT development staff extensive access creates a high risk that a fraudulent or unauthorized transaction could occur and be concealed.

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective access controls over mainframe production information systems.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding. The Departments informed us that access rights for staff in both Departments have been analyzed and updated in a special project completed since November 2003. Also, both Departments will continue to work together to establish policies and procedures, based on business risk assessments, to limit access to mainframe production information systems by March 2005.

FINDING

6. Program and Data Change Controls

The Department of State and the Department of Information Technology had not established effective program and data change controls. As a result, management did not have sufficient control to reduce the risk of unauthorized program and data changes to a reasonable level.

Our review of the program change control process disclosed:

a. The Departments had not established controls to ensure that only authorized program changes or data fixes were initiated.

   We noted that the Department of State did not identify the business owners or require the business owners to document authorization for all program changes or data fixes. Without a well-defined process to ensure that only

authorized changes are initiated, the Departments cannot ensure that programmers make only authorized program changes.

b. The Departments had not established controls to ensure that only authorized, tested, and documented program changes or data fixes were moved into production.

   Management did not identify or define the requirements to approve or release program changes or data fixes. Without a well-defined process, management cannot be assured that only authorized, tested, and documented changes to the information systems are accepted into production.

c. The Departments had not established effective controls to ensure the security and integrity of program versions.

   Programmers were not required to notify management when multiple copies of the same program were checked out for maintenance. This complicates the coordination of changes to the program. If not handled properly, an older version of the program could be moved back into production that would unintentionally reverse a previously approved change. Further, management did not check to ensure version control was maintained during its review of program changes.

d. The Departments had not granted access and authorization capability in the program change control system based on job function.

   IT staff had access beyond what was needed for their job function. Limiting IT staff to the access needed to perform job functions reduces the risk of unauthorized activity that could affect the integrity of mainframe application programs and data.

The Departments should establish clear and separate assignments of responsibility and accountability for planning, managing, and controlling changes to programs and data in the Department of State's information systems.

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective program and data change controls.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding. The Departments informed us that procedures now require that only project managers, assigned by the business owner, have the authority to authorize "project-related" program releases. In addition, the Departments will review and revise additional procedures that ensure appropriate controls are maintained over program and data changes by October 2004.

GLOSSARY

Control Objectives for Information and Related Technology (COBIT) control framework

In April 1996, the Information Systems Audit and Control Foundation (ISACF), a private not-for-profit organization, developed an internal control framework to manage, use, and audit information technology. The framework (referred to as COBIT) consists of 34 high-level control objectives associated with primary information technology processes, grouped into four domains. The four domains are planning and organization, acquisition and implementation, delivery and support, and monitoring.

The basic philosophy of the COBIT framework is to center the need for internal controls over information technology processes according to a natural grouping of common information technology processes. The framework is based on the concept that management must first achieve a complete understanding of the department's business processes before it can effectively develop, manage, and audit the processes for implementing information and related technology solutions. The framework is based on the underlying assumption that a department's core business processes drive the need for implementing information and related technology. Control objectives define the criteria that must be met to ensure delivery of technology solutions that meet the department's business requirements.

DMB

Department of Management and Budget.

effectiveness

Program success in achieving mission and goals.

Evaluation of Internal Controls - A General Framework and System of Reporting

The General Framework provides the basic structure for planning and conducting evaluations of a department's internal control structure with references to "evaluation tool sets" that are constructed using the same concepts. Departments are encouraged to obtain, review, and modify

these evaluation tools to best address the unique requirements of each department's environment.

Evaluation of Internal Controls - A General Framework and System of Reporting is a comprehensive revision to the guidance that was last issued in 1990. This new guidance is based upon terminology and concepts set forth in the report entitled "*Internal Control-Integrated Framework*," which was prepared by the Committee of Sponsoring Organizations of the Treadway Commission (often referred to as "COSO"). COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control, and corporate governance.

incompatible For internal control purposes, functions are considered to be incompatible if their performance by one person places that person in a position to both commit and conceal fraud or error.

internal control The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.

IT information technology.

IT development staff Computer programmers, systems analysts, and other persons responsible for developing business application systems.

material condition A reportable condition that could impair the ability of management to operate a program in an effective and

efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.

mission — The agency's main purpose or the reason that the agency was established.

performance audit — An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.